

To whom it may concern:

I am writing to oppose certain parts of the Commission's proposed rule concerning "Equipment Authorization and Electronic Labeling for Wireless Devices", which, though well-intentioned, will chill innovation in the wireless space and result in reduced security for end users.

Specifically, section 2.1033 paragraph 4(i) of the proposed rule states:

*"For devices including modular transmitters which are software defined radios and use software to control the radio or other parameters subject to the Commission's rules, the description must include details of the equipment's capabilities for software modification and upgradeability, including all frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, whether or not the device will be initially marketed with all modes enabled. The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation. Manufacturers must describe the methods used in the device to secure the software in their application for equipment authorization and must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters. The applicant must provide an attestation that only permissible modes of operation may be selected by a user."*

Regardless of the Commission's intentions, this language is likely to result in manufacturers adopting technology to prohibit the installation of any modified software on affected devices, even software which does not affect the intended operation of the radio in any way.

As the market for consumer electronic devices is a global one, manufacturers are very likely to continue to design radio hardware that is physically capable of operating in modes that, while not permitted in the United States, are available for use elsewhere in the world; access to those modes will, as today, be controlled by parameters provided by software.

With this proposed rule, manufacturers will have to choose between (1) including hardware in their radios to verify software-loaded parameters and then loading US-specific keys or other restrictions into US-market-bound devices, adding to the cost of components and the cost/complexity of manufacturing; or (2) preventing unauthorized parameters from being loaded by blocking software modifications entirely, including modifications entirely unrelated to radio functionality. This scenario is not hypothetical; manufacturers of wireless devices are already restricting software modification on devices as a result of the Commission's earlier rules regarding U-NII band radios.

Restricting software modifications to wireless devices will have a chilling effect on innovative projects that rely on the availability of user-modifiable wireless devices, such as:

- CeroWrt (<http://www.bufferbloat.net/projects/cerowrt>), wireless router software used for researching solutions to the pervasive problem of "bufferbloat", which causes extreme latency on congested networks;

- Comcast's test deployment of the next-generation IPv6 protocol to home networks, which built on top of OpenWrt's open-source community software for user-modifiable wireless routers (<http://www.comcast6.net/index.php/8-ipv6-trial-news-and-information/42-comcast-donates-additional-ipv6-open-source-software>); and
- The Commission's own Measuring Broadband America software for collecting data on the quality of fixed broadband connections, also based on OpenWrt wireless router software (<https://www.fcc.gov/encyclopedia/measuring-broadband-america-measuring-fixed-broadband>).

In addition, the fast-moving nature of the consumer electronics market results in many manufacturers quickly abandoning support for devices on the market as they move on to producing newer devices. This results in a large installed base of devices with known, unfixed security vulnerabilities (<http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>); restrictions on software modifications to these devices would worsen this problem by preventing end users from fixing these vulnerabilities themselves.

While the Commission's goals of simplifying the certification process for wireless devices and reducing misuse of shared wireless spectrum are laudable, they should not result in new barriers to innovation in the fast-moving wireless space or leave end users stuck with devices with unfixable security vulnerabilities. I urge the Commission to ensure that its final rule preserves innovation and protects online safety by making it easier for wireless devices allowing installation of user-modified software to pass certification.

Sincerely,

Steven Luo